Attorney Docket No. SKY03009

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	**Mail Stop Appeal Brief - Patents**
	)	
Gagan PURANIK et al.	)	Group Art Unit: 2137
	)	
Application No.: 10/758,199	)	Examiner: M. Nguyen
	)	
Filed: January 16, 2004	)	
	)	
For: METHOD AND SYSTEM FOR SECURED WIRELESS DATA TRANSMISSION TO AND FROM A REMOTE DEVICE	)	

APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Wind3ow, Mail Stop Appeal Brief - Patents
Randolph Building
401 Dulany Street
Alexandria, Virginia 22314

Sir:

This Appeal Brief is submitted in response to the final Office Action mailed March 24, 2008 and in support of the Notice of Appeal filed June 24, 2008.

I. REAL PARTY IN INTEREST

The real party in interest of the present application, solely for purposes of identifying and avoiding potential conflicts of interest by board members due to working in matters in which the member has a financial interest, is Verizon Communications Inc. and its subsidiary companies, which currently include Verizon Business Global, LLC

(formerly MCI, LLC) and Cellco Partnership (doing business as Verizon Wireless, and which includes as a minority partner affiliates of Vodafone Group Plc). Verizon Communications Inc. or one of its subsidiary companies is an assignee of record of the present application.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals, interferences or judicial proceedings.

III. STATUS OF CLAIMS

Claims 1-8 and 20-27 are pending in this application. Claims 1-8 and 20-27 were finally rejected in the Office Action dated March 24, 2008, and are the subject of the present appeal. Claims 9-19 and 28-33 were previously canceled without prejudice or disclaimer. Claims 1-8 and 20-27 are reproduced in the Claim Appendix of this Appeal Brief.

IV. STATUS OF AMENDMENTS

No Amendment has been filed subsequent to the final Office Action mailed March 24, 2008. Appellants did, however, file a Request for Reconsideration on May 20, 2008. A subsequent Advisory Action, dated June 4, 2008 indicated that the Request for Reconsideration was not persuasive.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Each of the independent claims involved in this appeal is recited below, followed

in parenthesis by examples of where support can be found in the specification and drawings for the claimed subject matter. In addition, each dependent claim argued separately below is also summarized in a similar manner.

Claim 1 recites: A method for secure message reception from a plurality of remote devices, comprising: receiving a message at a controller (e.g., 605, Fig. 6A; page 14, lines 7-18); obtaining, by the controller, a reverse channel address associated with the received message (e.g., 610, Fig. 6A; page 14, lines 7-18); determining, by the controller, whether the received message is associated with at least one of the remote devices (e.g., 625, Fig. 6A; page 14, lines 7-18); forwarding the message and the reverse channel address to a routing server when the message is associated with the at least one of the remote devices (e.g., 635, Fig. 6A; page 14, lines 7-18); determining, by the routing server, a destination address for the received message based on the reverse channel address (e.g., 670, Fig. 6B; page 14, lines 19-28); and routing the received message to the destination address (e.g., 675, Fig. 6B; page 14, lines 19-28).

Claim 6 recites: The method of claim 1, wherein determining the destination address further comprises: determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server (e.g., page 14, lines 19-28).

Claim 7 recites: The method of claim 6, wherein the received message is routed to the hosted crypto server (e.g., page 14, lines 19-28).

Claim 8 recites: The method of claim 6, wherein the received message is routed to the enterprise crypto server (e.g., page 14, lines 19-28).

Claim 20 recites: An apparatus for secure message reception from a plurality of

remote devices, comprising: means for receiving a message at a controller (e.g., 605, Fig. 6A; page 14, lines 7-18); means for obtaining, by the controller, a reverse channel address associated with the received message (e.g., 610, Fig. 6A; page 14, lines 7-18); means for determining, by the controller, whether the received message is associated with at least one of the remote devices (e.g., 625, Fig. 6A; page 14, lines 7-18); means for forwarding the message and the reverse channel address to a routing server when the message is associated with the at least one of the remote devices (e.g., 635, Fig. 6A; page 14, lines 7-18); means for determining, by the routing server, a destination address for the received message based on the reverse channel address (e.g., 670, Fig. 6B; page 14, lines 19-28); and means for routing the received message to the destination address (e.g., 675, Fig. 6B; page 14, lines 19-28).

Claim 25 recites: The apparatus of claim 20, wherein the means for determining the destination address further comprises: means for determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server (e.g., page 14, lines 19-28).

Claim 26 recites: The apparatus of claim 25, wherein the received message is routed to the hosted crypto server (e.g., page 14, lines 19-28).

Claim 27 recites: The apparatus of claim 25, wherein the received message is routed to the enterprise crypto server (e.g., page 14, lines 19-28).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1, 3-8, 20, and 22-27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over FARLEY et al. (U.S. Patent Application Publication No.

2006/0018293) in view of MOLES et al. (U.S. Patent No. 7,024,557).

B. Claims 2 and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over FARLEY et al. in view of MOLES et al. and further in view of BIMS et al. (U.S. Patent No. 6,259,911).

VII. ARGUMENTS

A. The rejection under 35 U.S.C. § 103 based on FARLEY et al. and MOLES et al. should be reversed.

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the Examiner must provide a factual basis to support the conclusion of obviousness. In re Warner, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967). Based upon the objective evidence of record, the Examiner is required to make the factual inquiries mandated by Graham v. John Deere Co., 86 S.Ct. 684, 383 U.S. 1, 148 USPQ 459 (1966). KSR International Co. v. Teleflex Inc., 550 U.S. ___, 127 S. Ct. 1727 (2007). The Examiner is also required to explain how and why one having ordinary skill in the art would have been realistically motivated to modify an applied reference and/or combine applied references to arrive at the claimed invention. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988).

1. Claims 1 and 3-5

With the above principles in mind, claim 1 recites a method for secure message reception from a plurality of remote devices. The method includes receiving a message

at a controller; obtaining, by the controller, a reverse channel address associated with the received message; determining, by the controller, whether the received message is associated with at least one of the remote devices; forwarding the message and the reverse channel address to a routing server when the message is associated with the at least one of the remote devices; determining, by the routing server, a destination address for the received message based on the reverse channel address; and routing the received message to the destination address. FARLEY et al. and MOLES et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, FARLEY et al. and MOLES et al. do not disclose or suggest forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 1. The Examiner relies on Fig. 7 and paragraphs 0094-0098 (which describe Fig. 7) of FARLEY et al. and Fig. 1, column 4, lines 7-13, column 5, lines 43-49 (which describes Fig. 1), and column 6, lines 13-21 of MOLES et al. as allegedly disclosing these features of claim 1 (final Office Action, pp. 3-4). Appellants respectfully disagree with the Examiner's interpretation of FARLEY et al. and MOLES et al.

At paragraphs 0094-0098, FARLEY et al. discloses forwarding a network message from a PC device to a server via a wireless link between a subscriber unit and a base station. This section of FARLEY et al. further discloses that both the base station and the subscriber unit simultaneously track each established session based on a 16-bit

L4 stream identifier tag that includes a source IP address, destination IP address, source port number, and destination port number. This section of FARLEY et al. does not disclose or suggest determining, at a routing server, a destination address for a received message based on a reverse channel address. Rather, at noted above, FARLEY et al. discloses that each session is assigned an L4 stream ID tag that includes a source IP address and a destination IP address. Therefore, this section of FARLEY et al. does not disclose or suggest forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 1. Rather, this section of FARLEY et al. clearly discloses that the information transmitted between the base station and the subscriber unit includes the destination address as part of the L4 stream ID tag.

At column 4, lines 7-13, MOLES et al. discloses:

> According to another embodiment of the present invention, the first controller is disposed in a mobile switching center of the wireless network. In other embodiments of the present invention, the first controller may be disposed in an interworking function unit of the wireless network, or may be partitioned between the mobile switching center and the interworking function unit.

This section of MOLES et al. discloses that a controller may be disposed in an interworking function unit of a wireless network or may be portioned between a mobile switching center and an interworking function unit. This section of MOLES et al. discloses a controller in a wireless network and does not have anything to do with determining a destination address for a received message based on a reverse channel address. Therefore, this section of MOLES et al. does not disclose or suggest forwarding a message and a reverse channel address to a routing server when the message is

associated with the at least one of a plurality of remote devices and determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 1.

At column 5, lines 43-49, MOLES et al. discloses:

> FIG. 1 illustrates a general overview of an exemplary wireless network 100 according to one embodiment of the present invention. The wireless telephone network 100 comprises a plurality of cell sites 121 123, each containing one of the base stations, BS 101, BS 102, or BS 103. Base stations 101 103 are operable to communicate with a plurality of mobile stations (MS) 111-114.

This section of MOLES et al. discloses a wireless telephone network that includes a plurality of cell sites that each contain a base station that are operable to communicate with a plurality of mobile stations. This section of MOLES et al. has nothing to do with determining a destination address for a received message based on a reverse channel address. Therefore, this section of MOLES et al. does not disclose or suggest forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 1.

At column 6, lines 13-21, MOLES et al. discloses:

> BS 101, BS 102 and BS 103 transfer voice and data signals between each other and the public telephone system (not shown) via communications line 131 and mobile switching center (MSC) 140. Mobile switching center 140 is well known to those skilled in the art. Mobile switching center 140 is a switching device that provides services and coordination between the subscribers in a wireless network and external networks, such as the public telephone system and/or the Internet.

This section of MOLES et al. discloses a mobile switching center that provides services and coordination between subscribers in a wireless network and external network, such as the public telephone system and/or the Internet. This section of MOLES et al. has

nothing to do with determining a destination address for a received message based on a reverse channel address. Therefore, this section of MOLES et al. does not disclose or suggest forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 1.

In response to similar arguments made in a previous response, in the Advisory Action, the Examiner alleges that FARLEY et al. "discloses the data traffic transmitted from the PC 12 towards the server 30 on the reverse link 50 direction and the data information generated by PC device 12 is based on a TCP/IP protocol" and relies on paragraph 0053 of FARLEY et al. for support (Advisory Action, pg. 2). Regardless of the validity of the Examiner's statement, generating information based on a TCP/IP protocol has nothing to do with determining a destination address for a received message based on a reverse channel address. In fact, FARLEY et al. discloses that generating information based on a TCP/IP protocol allows a PC device to access digital information such as web pages available on the Internet (paragraph 0053). Accessing web pages available on the Internet is in no way equivalent to determining a destination address for a received message based on a reverse channel address. Therefore, this section of FARLEY et al. does not disclose or suggest forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 1.

The Examiner further alleges that FARLEY et al. discloses that "the reverse link

includes different types of channels and is used to carry payload data from the subscriber unit to the base station," and relies on paragraphs 0056-0058 of FARLEY for support (Advisory Action, pg. 2). Regardless of the validity of the Examiner's statement, carrying payload data from a subscriber unit to a base station is in no way equivalent to determining a destination address for a received message based on a reverse channel address. Therefore, this section of FARLEY et al. does not disclose or suggest forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 1.

The Examiner further states that FARLEY et al. "discloses the JACK channel for carrying messages over the reverse channel…which further discloses to have the base station identifies the destination IP address for an L4 ACK message to reconstruct and forwards the network message accordingly," and relies on paragraphs 0094-0098 of FARLEY et al. for support (Advisory Action, pg. 2). However, as noted above, FARLEY et al. discloses that each session is assigned an L4 stream ID tag that includes a source IP address and a destination IP address. Therefore, this section of FARLEY et al. does not disclose or suggest forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 1. Rather, this section of FARLEY et al. clearly discloses that the information transmitted between the base station and the subscriber unit includes the destination address as part of the L4

stream ID tag.

For at least the foregoing reasons, Appellants submit that the rejection of claim 1 under 35 U.S.C. § 103(a) based on FARLEY et al. and MOLES et al. is improper. Accordingly, Appellants request that the rejection be reversed.

Claims 3-5 depend from claim 1. Therefore, Appellants request that the rejection of claims 3-5 be reversed for at least the reasons given above with respect to claim 1.

2. Claim 6

Claim 6 depends from claim 1. Therefore, Appellants request that the rejection of claim 6 be reversed for at least the reasons given above with respect to claim 1. Moreover, claim 6 recites additional features not disclosed or suggested by FARLEY et al. and MOLES et al.

For example, claim 6 recites determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server. The Examiner relies on column 8, line 59 – column 9, line 8 of MOLES et al. as allegedly disclosing this feature (final Office Action, pg. 5). Appellants respectfully disagree with the Examiner's interpretation of MOLES et al.

At column 8, line 59 – column 9, line 8, MOLES et al. discloses:

> Authentication controller 260 initially stores incoming data from MS 112 and compares the received SSD information with SSD information retrieved from HLR 155. If authentication controller 260 determines that the received SSD information from MS 112 is valid, then authentication controller 260 examines other data stored in HLR 155, such as NAM data and billing information, to determine if MS 112 has been provisioned. If authentication controller 260 verifies that MS 112 is properly provisioned, the voice/data call is transferred to MSC 140 for normal call processing. If authentication controller 260 determines that MS 112 has not been previously provisioned (i.e., no billing information, no NAM data, etc.), authentication controller 260 transfers all incoming IP packets to provisioning security controller 265 for encryption and transfer to provisioning

> server 160 through MSC 140 and Internet 165, as described below in greater detail.

This section of MOLES et al. discloses that, if a mobile station has been provisioned, a voice/data call is transferred for normal processing and if the mobile station has not been provisioned, an authentication controller transfers all incoming IP packets to a provisioning security controller for encryption and transfer to a provisioning server. This section of MOLES et al. is not related to and does not mention a hosted crypto server or an enterprise crypto server. Therefore, this section of MOLES et al. cannot disclose or suggest determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server, as recited in claim 6.

In response to similar arguments made in a previous response, the Examiner alleges that "Moles discloses provisioning server has the key to the encryption algorithm used by base station, provisioning server is able to process legitimate service provisioning requests from mobile station, as such provisioning server is a hosted crypto server or an enterprise crypto server" and relies on column 10, lines 5-8 of MOLES et al. for support (final Office Action, pg. 2). Appellants respectfully disagree with the Examiner's allegation.

At column 10, lines 5-8, MOLES et al. discloses that the provisioning server has the key to an encryption algorithm used by a base station. Having a key to an encryption algorithm used by a base station is in no way equivalent to determining whether the receive message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server. Neither this section, nor any other section, of MOLES et al. discloses a hosted crypto server or an enterprise crypto server. Therefore,

this section of MOLES et al. does not disclose or suggest determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server, as recited in claim 6.

For at least these additional reasons, Appellants submit that the rejection of claim 6 under 35 U.S.C. § 103(a) based on FARLEY et al. and MOLES et al. is improper. Accordingly, Appellants request that the rejection be reversed.

3. Claim 7

Claim 7 depends from claim 6. Therefore, Appellants request that the rejection of claim 7 be reversed for at least the reasons given above with respect to claim 6. Moreover, claim 7 recites additional features not disclosed or suggested by FARLEY et al. and MOLES et al.

For example, claim 7 recites that the received message is routed to the hosted crypto server. The Examiner relies on column 9, lines 6-8 and 19-22 of MOLES et al. for support (final Office Action, pp. 5-6). Appellants respectfully disagree with the Examiner's interpretation of MOLES et al.

At column 9, lines 6-8, MOLES et al. discloses that if a mobile station has not been previously provisioned, all incoming IP packets are transferred to a provisioning security controller for encryption and then transferred to provisioning server 160, a system-wide central server. Automatically transferring encrypted packets to a central server when a mobile station has not been provisioned is in no way equivalent to routing a received message to the hosted crypto server. Therefore, this section of MOLES et al. does not disclose or suggest that the received message is routed to the hosted crypto

server, as recited in claim 7.

At column 9, lines 19-22, MOLES et al. discloses that, if a mobile station has dialed a special telephone number reserved for service provisioning, all incoming IP packets from the mobile station may be transferred to a provisioning security controller for encryption and then transferred to provisioning server 160. Provisioning server 160 is a system-wide central server (column 7, lines 1-3) and is not equivalent to the hosted crypto server. Therefore, this section of MOLES et al. does not disclose or suggest that the received message is routed to the hosted crypto server, as recited in claim 7.

For at least these additional reasons, Appellants submit that the rejection of claim 7 under 35 U.S.C. § 103(a) based on FARLEY et al. and MOLES et al. is improper. Accordingly, Appellants request that the rejection be reversed.

4. Claim 8

Claim 8 depends from claim 6. Therefore, Appellants request that the rejection of claim 8 be reversed for at least the reasons given above with respect to claim 6. Moreover, claim 8 recites additional features not disclosed or suggested by FARLEY et al. and MOLES et al.

For example, claim 8 recites that the received message is routed to the enterprise crypto server. The Examiner relies on column 9, lines 6-8 and 19-22 of MOLES et al. for support (final Office Action, pp. 5-6). Appellants respectfully disagree with the Examiner's interpretation of MOLES et al.

At column 9, lines 6-8, MOLES et al. discloses that if a mobile station has not been previously provisioned, all incoming IP packets are transferred to a provisioning

security controller for encryption and then transferred to provisioning server 160, a system-wide central server. Automatically transferring encrypted packets to a central server when a mobile station has not been provisioned is in no way equivalent to routing a received message to the enterprise crypto server. Therefore, this section of MOLES et al. does not disclose or suggest that the received message is routed to the enterprise crypto server, as recited in claim 8.

At column 9, lines 19-22, MOLES et al. discloses that, if a mobile station has dialed a special telephone number reserved for service provisioning, all incoming IP packets from the mobile station may be transferred to a provisioning security controller for encryption and then transferred to provisioning server 160. Provisioning server 160 is a system-wide central server (column 7, lines 1-3) and is not equivalent to the enterprise crypto server. Therefore, this section of MOLES et al. does not disclose or suggest that the received message is routed to the enterprise crypto server, as recited in claim 8.

For at least these additional reasons, Appellants submit that the rejection of claim 8 under 35 U.S.C. § 103(a) based on FARLEY et al. and MOLES et al. is improper. Accordingly, Appellants request that the rejection be reversed.

5. Claims 20 and 22-24

Independent claim 20 recites an apparatus for secure message reception from a plurality of remote devices. The apparatus comprises means for receiving a message at a controller; means for obtaining, by the controller, a reverse channel address associated with the received message; means for determining, by the controller, whether the received message is associated with at least one of the remote devices; means for

forwarding the message and the reverse channel address to a routing server when the message is associated with the at least one of the remote devices; means for determining, by the routing server, a destination address for the received message based on the reverse channel address; and means for routing the received message to the destination address. FARLEY et al. and MOLES et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, FARLEY et al. and MOLES et al. do not disclose or suggest means for forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and means for determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 20. The Examiner relies on Fig. 7 and paragraphs 0094-0098 (which describe Fig. 7) of FARLEY et al. and Fig. 1, column 4, lines 7-13, column 5, lines 43-49 (which describes Fig. 1), and column 6, lines 13-21 of MOLES et al. as allegedly disclosing these features of claim 20 (final Office Action, pp. 3-4). Appellants respectfully disagree with the Examiner's interpretation of FARLEY et al. and MOLES et al.

At paragraphs 0094-0098, FARLEY et al. discloses forwarding a network message from a PC device to a server via a wireless link between a subscriber unit and a base station. This section of FARLEY et al. further discloses that both the base station and the subscriber unit simultaneously track each established session based on a 16-bit L4 stream identifier tag that includes a source IP address, destination IP address, source port number, and destination port number. This section of FARLEY et al. does not disclose or suggest means for determining, at a routing server, a destination address for a

received message based on a reverse channel address. Rather, as noted above, FARLEY et al. discloses that each session is assigned an L4 stream ID tag that includes a source IP address and a destination IP address. Therefore, this section of FARLEY et al. does not disclose or suggest means for forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and means for determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 20. Rather, this section of FARLEY et al. clearly discloses that the information transmitted between the base station and the subscriber unit includes the destination address as part of the L4 stream ID tag.

At column 4, lines 7-13, MOLES et al. discloses:

> According to another embodiment of the present invention, the first controller is disposed in a mobile switching center of the wireless network. In other embodiments of the present invention, the first controller may be disposed in an interworking function unit of the wireless network, or may be partitioned between the mobile switching center and the interworking function unit.

This section of MOLES et al. discloses that a controller may be disposed in an interworking function unit of a wireless network or may be portioned between a mobile switching center and an interworking function unit. This section of MOLES et al. discloses a controller in a wireless network and does not have anything to do with means for determining a destination address for a received message based on a reverse channel address. Therefore, this section of MOLES et al. does not disclose or suggest means for forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and means for determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 20.

At column 5, lines 43-49, MOLES et al. discloses:

> FIG. 1 illustrates a general overview of an exemplary wireless network 100 according to one embodiment of the present invention. The wireless telephone network 100 comprises a plurality of cell sites 121 123, each containing one of the base stations, BS 101, BS 102, or BS 103. Base stations 101 103 are operable to communicate with a plurality of mobile stations (MS) 111-114.

This section of MOLES et al. discloses a wireless telephone network that includes a plurality of cell sites that each contain a base station that are operable to communicate with a plurality of mobile stations. This section of MOLES et al. has nothing to do with means for determining a destination address for a received message based on a reverse channel address. Therefore, this section of MOLES et al. does not disclose or suggest means for forwarding a message and a reverse channel address to a routing server when the message is associated with the at least one of a plurality of remote devices and means for determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 20.

At column 6, lines 13-21, MOLES et al. discloses:

> BS 101, BS 102 and BS 103 transfer voice and data signals between each other and the public telephone system (not shown) via communications line 131 and mobile switching center (MSC) 140. Mobile switching center 140 is well known to those skilled in the art. Mobile switching center 140 is a switching device that provides services and coordination between the subscribers in a wireless network and external networks, such as the public telephone system and/or the Internet.

This section of MOLES et al. discloses a mobile switching center that provides services and coordination between subscribers in a wireless network and external network, such as the public telephone system and/or the Internet. This section of MOLES et al. has nothing to do with means for determining a destination address for a received message based on a reverse channel address. Therefore, this section of MOLES et al. does not disclose or suggest means for forwarding a message and a reverse channel address to a

routing server when the message is associated with the at least one of a plurality of remote devices and means for determining, by the routing server, a destination address for the received message based on the reverse channel address, as recited in claim 20.

For at least the foregoing reasons, Appellants submit that the rejection of claim 20 under 35 U.S.C. § 103(a) based on FARLEY et al. and MOLES et al. is improper. Accordingly, Appellants request that the rejection be reversed.

Claims 22-24 depend from claim 20. Therefore, Appellants request that the rejection of claims 22-24 be reversed for at least the reasons given above with respect to claim 20.

6. Claim 25

Claim 25 depends from claim 20. Therefore, Appellants request that the rejection of claim 25 be reversed for at least the reasons given above with respect to claim 20. Moreover, claim 25 recites additional features not disclosed or suggested by FARLEY et al. and MOLES et al.

For example, claim 25 recites means for determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server. The Examiner relies on column 8, line 59 – column 9, line 8 of MOLES et al. as allegedly disclosing this feature (final Office Action, pp. 5-6). Appellants respectfully disagree with the Examiner's interpretation of MOLES et al.

At column 8, line 59 – column 9, line 8, MOLES et al. discloses:

> Authentication controller 260 initially stores incoming data from MS 112 and compares the received SSD information with SSD information retrieved from HLR 155. If authentication controller 260 determines that the received SSD information from MS 112 is valid, then authentication controller 260 examines

> other data stored in HLR 155, such as NAM data and billing information, to determine if MS 112 has been provisioned. If authentication controller 260 verifies that MS 112 is properly provisioned, the voice/data call is transferred to MSC 140 for normal call processing. If authentication controller 260 determines that MS 112 has not been previously provisioned (i.e., no billing information, no NAM data, etc.), authentication controller 260 transfers all incoming IP packets to provisioning security controller 265 for encryption and transfer to provisioning server 160 through MSC 140 and Internet 165, as described below in greater detail.

This section of MOLES et al. discloses that, if a mobile station has been provisioned, a voice/data call is transferred for normal processing and if the mobile station has not been provisioned, an authentication controller transfers all incoming IP packets to a provisioning security controller for encryption and transfer to a provisioning server. This section of MOLES et al. is not related to and does not mention a hosted crypto server or an enterprise crypto server. Therefore, this section of MOLES et al. cannot disclose or suggest means for determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server, as recited in claim 25.

In response to similar arguments made in a previous response, the Examiner alleges that "Moles discloses provisioning server has the key to the encryption algorithm used by base station, provisioning server is able to process legitimate service provisioning requests from mobile station, as such provisioning server is a hosted crypto server or an enterprise crypto server" and relies on column 10, lines 5-8 of MOLES et al. for support (final Office Action, pg. 2). Appellants respectfully disagree with the Examiner's allegation.

At column 10, lines 5-8, MOLES et al. discloses that the provisioning server has the key to an encryption algorithm used by a base station. Having a key to an encryption algorithm used by a base station is in no way equivalent to determining whether the

receive message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server. Neither this section, nor any other section, of MOLES et al. discloses a hosted crypto server or an enterprise crypto server. Therefore, this section of MOLES et al. does not disclose or suggest means for determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server, as recited in claim 25.

For at least these additional reasons, Appellants submit that the rejection of claim 25 under 35 U.S.C. § 103(a) based on FARLEY et al. and MOLES et al. is improper. Accordingly, Appellants request that the rejection be reversed.

7. Claim 26

Claim 26 depends from claim 25. Therefore, Appellants request that the rejection of claim 26 be reversed for at least the reasons given above with respect to claim 25. Moreover, claim 26 recites additional features not disclosed or suggested by FARLEY et al. and MOLES et al.

For example, claim 26 recites that the received message is routed to the hosted crypto server. The Examiner relies on column 9, lines 6-8 and 19-22 of MOLES et al. for support (final Office Action, pp. 5-6). Appellants respectfully disagree with the Examiner's interpretation of MOLES et al.

At column 9, lines 6-8, MOLES et al. discloses that if a mobile station has not been previously provisioned, all incoming IP packets are transferred to a provisioning security controller for encryption and then transferred to provisioning server 160, a system-wide central server. Automatically transferring encrypted packets to a central

server when a mobile station has not been provisioned is in no way equivalent to routing a received message to the hosted crypto server. Therefore, this section of MOLES et al. does not disclose or suggest that the received message is routed to the hosted crypto server, as recited in claim 26.

At column 9, lines 19-22, MOLES et al. discloses that, if a mobile station has dialed a special telephone number reserved for service provisioning, all incoming IP packets from the mobile station may be transferred to a provisioning security controller for encryption and then transferred to provisioning server 160. Provisioning server 160 is a system-wide central server (column 7, lines 1-3) and is not equivalent to the hosted crypto server. Therefore, this section of MOLES et al. does not disclose or suggest that the received message is routed to the hosted crypto server, as recited in claim 26.

For at least these additional reasons, Appellants submit that the rejection of claim 26 under 35 U.S.C. § 103(a) based on FARLEY et al. and MOLES et al. is improper. Accordingly, Appellants request that the rejection be reversed.

8. Claim 27

Claim 27 depends from claim 25. Therefore, Appellants request that the rejection of claim 27 be reversed for at least the reasons given above with respect to claim 25. Moreover, claim 27 recites additional features not disclosed or suggested by FARLEY et al. and MOLES et al.

For example, claim 27 recites that the received message is routed to the enterprise crypto server. The Examiner relies on column 9, lines 6-8 and 19-22 of MOLES et al. for support (final Office Action, pp. 5-6). Appellants respectfully disagree with the

Examiner's interpretation of MOLES et al.

At column 9, lines 6-8, MOLES et al. discloses that if a mobile station has not been previously provisioned, all incoming IP packets are transferred to a provisioning security controller for encryption and then transferred to provisioning server 160, a system-wide central server. Automatically transferring encrypted packets to a central server when a mobile station has not been provisioned is in no way equivalent to routing a received message to the enterprise crypto server. Therefore, this section of MOLES et al. does not disclose or suggest that the received message is routed to the enterprise crypto server, as recited in claim 27.

At column 9, lines 19-22, MOLES et al. discloses that, if a mobile station has dialed a special telephone number reserved for service provisioning, all incoming IP packets from the mobile station may be transferred to a provisioning security controller for encryption and then transferred to provisioning server 160. Provisioning server 160 is a system-wide central server (column 7, lines 1-3) and is not equivalent to the enterprise crypto server. Therefore, this section of MOLES et al. does not disclose or suggest that the received message is routed to the enterprise crypto server, as recited in claim 27.

For at least these additional reasons, Appellants submit that the rejection of claim 27 under 35 U.S.C. § 103(a) based on FARLEY et al. and MOLES et al. is improper. Accordingly, Appellants request that the rejection be reversed.

B. The rejection under 35 U.S.C. § 103 based on FARLEY et al., MOLES et al., and BIMS et al. should be reversed.

1. Claim 2

Claim 2 depends from claim 1. Without acquiescing in the Examiner's rejection of claim 2, Appellants submit that the disclosure of BIMS et al. does not remedy the deficiencies in the disclosures of FARLEY et al. and MOLES et al. set forth above with respect to claim 1. Therefore, Appellants request that the rejection of claim 2 be reversed for at least the reasons given above with respect to claim 1.

2. Claim 21

Claim 21 depends from claim 20. Without acquiescing in the Examiner's rejection of claim 21, Appellants submit that the disclosure of BIMS et al. does not remedy the deficiencies in the disclosures of FARLEY et al. and MOLES et al. set forth above with respect to claim 20. Therefore, Appellants request that the rejection of claim 21 be reversed for at least the reasons given above with respect to claim 20.

VIII. CONCLUSION

In view of the foregoing arguments, Appellants respectfully solicit the Honorable Board to reverse the Examiner's rejections of claims 1-8 and 20-27.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /Meagan S. Walling, Reg. No. 60,112/
Meagan S. Walling
Reg. No. 60,112

Date: August 20, 2008

11350 Random Hills Road
Suite 600
Fairfax, VA 22030
Telephone: (571) 432-0800
Facsimile: (571) 432-0808

CUSTOMER NUMBER: 25537

IX. APPENDIX

1. A method for secure message reception from a plurality of remote devices, comprising:

receiving a message at a controller;

obtaining, by the controller, a reverse channel address associated with the received message;

determining, by the controller, whether the received message is associated with at least one of the remote devices;

forwarding the message and the reverse channel address to a routing server when the message is associated with the at least one of the remote devices;

determining, by the routing server, a destination address for the received message based on the reverse channel address; and

routing the received message to the destination address.

2. The method of claim 1, wherein a communications protocol employed to transmit the received message is a ReFLEX protocol.

3. The method of claim 1, wherein determining whether the received message is associated with at least one of the remote devices further comprises:

reviewing header information in the received message.

4. The method of claim 3, wherein determining the destination address further comprises:

retrieving a remote device profile based upon the obtained reverse channel address.

5. The method of claim 4, wherein determining the destination address further comprises:

obtaining the destination address from a remote device.

6. The method of claim 1, wherein determining the destination address further comprises:

determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server.

7. The method of claim 6, wherein the received message is routed to the hosted crypto server.

8. The method of claim 6, wherein the received message is routed to the enterprise crypto server.

20. An apparatus for secure message reception from a plurality of remote devices, comprising:

means for receiving a message at a controller;

measns for obtaining, by the controller, a reverse channel address associated with the received message;

means for determining, by the controller, whether the received message is associated with at least one of the remote devices;

means for forwarding the message and the reverse channel address to a routing server when the message is associated with the at least one of the remote devices;

means for determining, by the routing server, a destination address for the received message based on the reverse channel address; and

means for routing the received message to the destination address.

21. The apparatus of claim 20, wherein a communications protocol employed to transmit the received message is a ReFLEX protocol.

22. The apparatus of claim 20, wherein the means for determining whether the received message is associated with at least one of the remote devices further comprises:

means for reviewing header information in the received message.

23. The apparatus of claim 3, wherein the means for determining the destination address further comprises:

means for retrieving a remote device profile based upon the obtained reverse channel address.

24. The apparatus of claim 23, wherein the means for determining the destination address further comprises:

means for obtaining the destination address from a remote device.

25. The apparatus of claim 20, wherein the means for determining the destination address further comprises:

means for determining whether the received message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server.

26. The apparatus of claim 25, wherein the received message is routed to the hosted crypto server.

27. The apparatus of claim 25, wherein the received message is routed to the enterprise crypto server.

X. EVIDENCE APPENDIX

None

XI. RELATED PROCEEDINGS APPENDIX

None